Public Spaces in the Digital Age

Eli Lehrer

The nature of public space in America has been thoroughly transformed since the beginning of the 21st century. Public squares, parks, movie theaters, restaurants, and shopping centers now compete with social-media sites, video-conferencing software, dating apps, entertainment platforms, and online mega-stores as the “places” where Americans work, shop, and socialize. The Covid-19 pandemic and associated lockdowns only accelerated the trend toward virtualization. As the country re-emerges from months of social distancing, it’s clear that at least some of the pandemic-era changes in our social lives are here to stay.

The sheer size and influence of the virtual public sphere make it inevitable that public policy will have to consider it. Facebook — where nearly 70% of American adults maintain personal profiles — has proven itself far more significant to the nation’s cultural life than the Mall of America, the Rose Bowl, or even the U.S. Capitol. No park or public forum receives nearly as much use as Twitter or Instagram, and no brick-and-mortar store attracts nearly as many customers as major e-commerce websites like Amazon and Wayfair.

While some on the ultra-libertarian end of the political spectrum might wish to see these virtual spaces remain government-free zones, there is little reason to think that policymakers or the public will tolerate an entirely hands-off approach in the long run. After all, securing and maintaining public spaces is an essential responsibility of government. With virtual spaces now serving as important public forums, the question policymakers should be asking is not whether the government should regulate them, but how these new public spaces can be regulated responsibly and effectively.

Eli Lehrer is co-founder and president of the R Street Institute.
With digital environments playing a more dominant role in American society, concerns over safety, ownership, and free speech have grown in tandem. Though these challenges may feel like Information Age novelties, they are fundamentally the same issues that have influenced our approach to public spaces for centuries. As policymakers set out to tame America’s nascent virtual public sphere, they would do well to consider how the conventions, laws, and principles that have worked so well in maintaining social order in our physical public spaces might apply in our virtual ones. Ultimately, it is these long-standing norms, rules, and practices that offer the best models for ensuring that some of America’s most important public spaces remain safe, vibrant, and accessible.

**Securing Virtual Space**

Of all the challenges presented by virtual public spaces, the most urgent is safety. Two decades after the internet came into widespread use, cyber-space has retained something of a Wild West feel. It isn’t always clear to the public which laws and norms will be reliably observed or enforced when they go online, and this fosters an environment of disorder and distrust. Despite the early efforts of law enforcement and government regulators, too many Americans don’t feel as secure as they should when they enter virtual public spaces.

Of course, when it comes to physical harm, virtual space is very safe compared to the physical world. While two people standing in a public park or shopping mall can injure or kill one another, even the most vicious disputes in virtual environments will never result in a broken bone — at least not directly. Nevertheless, a strong sense of danger exists in virtual space.

This is especially the case with regard to child predators. But these widely discussed and often sensationalized incidents are far from the most common online crimes. The most pervasive threat to law and order in the virtual sphere is minor financial crime, as any internet user can attest. Obvious scams arrive in almost every email inbox on a regular basis, and nearly everyone who maintains an account on a major social-media platform has been approached by a fraudster.

The major safety problem in virtual space, then, is the one social scientists like George Kelling and Wesley Skogan identified in their landmark research on urban crime in the 1980s. At the time, most
researchers and police officers focused the bulk of their attention on studying and addressing serious violent crime. But in 1982, Kelling, along with political scientist James Wilson, published a novel theory regarding the upstream causes of neighborhood decay. They posited that superficial signs of chaos and lawlessness, like broken windows in a building, create a culture of incivility within a community, and that this prevailing sense of disorder gives those who are criminally inclined “permission” to commit more crimes. This, in turn, fuels an atmosphere of distrust and fear, and ultimately leads to a vicious cycle of social turmoil and criminal activity.

During the decades that followed, “broken windows” policing—whereby police crack down on disorderly behaviors like panhandling, public drinking, and street prostitution in an attempt to prevent more serious crimes downstream—was highly influential among police departments. While such tactics are far from the panacea some media accounts have claimed, there is evidence that policing minor violations in public spaces modestly reduces crime, increases the sense of safety in a shared environment, and makes those areas less unpleasant in general. These physical spaces, even in relatively unsafe cities, are typically secure (at least during the day), and the safest places of any size usually have some sort of security presence to maintain order. If they are doing their jobs properly, police officers standing in a city square or security guards patrolling a mall make very few custodial arrests. Instead, they deter crime through their presence and, by intervening early on, can prevent bad behavior from turning into serious crime.

Yet their equivalents don’t exist in virtual space. Instead, the overwhelming bulk of law-enforcement resources targets two of the most serious crimes: human trafficking and the sexual exploitation of children. Sex offenders comprise the third-largest group of federal inmates in America, and a majority of those serving time for such offenses were arrested for violating laws related to child pornography on the internet. Pennsylvania, one of the states that compiles its own cybercrime statistics, says that about 70% of its cybercrime cases involve such materials; states like Kentucky and Illinois offer similar assessments.

Efforts to combat online sex crimes are obviously worthwhile, just as efforts to address serious violent crimes in the decades leading up to the 1980s were overwhelmingly valuable. But the problem is that hardly any
other criminal act committed in cyberspace is ever punished, or even investigated. In 2019, internet fraud led to cumulative losses of $1.9 billion, and yet it’s hard to find anyone in a position of authority who takes it seriously. Local police departments often go after child predators outside of their jurisdictions, yet few would earnestly investigate an in-state online act of fraud that deprived a senior citizen of his Social Security check. It’s indicative that the Federal Trade Commission — an entity without criminal law-enforcement powers — is the primary tracker of online fraud crimes.

To effect the changes required, no new laws are necessary, nor are significant new resources. What our virtual public spaces need is more reliable enforcement of existing laws by state actors at all levels of government, along with a willingness to devote resources to combatting non-sex crimes. Police should be at least as attentive to such crimes committed online as they are to those committed on the street. In short, it’s time to start repairing “broken windows” in virtual spaces.

The private parties who own most online spaces should also do more to ensure users’ security. Microsoft, Alphabet, and online-dating giant Match Group should be considered just as responsible for their users’ safety as the owners of malls and movie theaters are for their patrons’ safety. These tech companies and their peers have safety and security departments, maintain significant professional trust, and employ law-enforcement veterans with cybercrime experience. Like owners of other public spaces, helping users feel safe is in the interest of these businesses as well.

What’s missing from the picture is a common standard of safety. In online spaces, behavior that makes people feel safe or unsafe is highly dependent on context. Vulgar abuse may be grounds for firing a worker who directs such cruelty at a colleague online, but it is expected from those who sign up for the “privilege” of being “roasted” on Reddit’s “r/RoastMe” forum. The same, of course, is true of physical spaces: Screaming insults at performers may be de rigueur at a professional wrestling match, but it will get one kicked out of the opera.

When it comes to online spaces, the appropriate range of behaviors is so large that no single industry-wide standard is feasible. Still, it is possible for tech companies to commit to some very basic duties that nearly all virtual spaces owe to their users. These might include care — content targeted at users shouldn’t be harmful to them, for example — and
loyalty—companies shouldn’t put profits ahead of users’ safety. Clear standards established by industry bodies based on age-old models (like the codes of medical or judicial ethics) and more recent ones (the comic-book industry’s code, or codes of conduct posted in malls) could go a long way toward making the virtual world feel safer to its billions of users.

In short, it’s time we start taking security in our virtual public spaces as seriously as we do in our physical public spaces. As is the case with the latter, this will require both public officials and private owners to play a role. If combined with a law-enforcement effort that takes all kinds of online crime seriously, users of platforms that can be held to safety promises would feel more secure, leading to a safer virtual environment overall.

PRIVATE OWNERSHIP, PUBLIC ACCESS

Somewhat counterintuitively, the great majority of public space in the physical world is privately owned. Americans don’t rely on local governments to provide malls, hotels, restaurants, movie theaters, cultural facilities, or most recreational areas. With some exceptions—mostly in the latter two categories—government efforts to run these spaces have a consistent record of failure. Even parks, which are automatically associated with the government in many minds, aren’t always public: In 2019, the most visited park in America was the privately run Magic Kingdom at Disney World, which brought in nearly twice as many people as the most visited national park.

So while the federal government owns vast stretches of essentially unusable land and maintains other areas for environmental and recreational purposes, the overwhelming majority of physical public spaces that people use day-to-day are, and always have been, privately owned. The public-use system that has evolved in the physical world combines protection of private ownership with assertive efforts by public officials to ensure equal access to these spaces. There is no reason the same standards can’t apply in virtual spaces.

Not everyone agrees, however. A dislike of too much private control over the digital environment has made for some unusual political bedfellows. In his most recent campaign for president, Senator Bernie Sanders called for both a publicly financed, politically controlled internet provider and price controls on whichever private providers survived competition with the public option. Though they are less open about
their demand for public control, both former president Donald Trump and former House speaker Newt Gingrich have argued for a national 5G network on security and global-competitiveness grounds. This past year, several Republican congressmen called for assertive government action to break up the Big Tech companies that own and manage most virtual public spaces.

Whatever one thinks of these suggestions—and even if some of the entities resulting from subsidies, nationalization, or breakups end up in nominally private hands—it’s hard to avoid the conclusion that they are likely to suffer from the same problems that plague public-sector efforts to run places like malls and hotels: insulation from market forces in their design, product offerings, and activities. For anyone who believes markets help firms make good decisions, nationalizing or dictating the precise activities of those who own virtual public spaces should be considered equivalent to government telling condominium developers exactly where to build, whom to rent to, and what to charge. Experience has borne out the absurdity of this approach: Government efforts to run broadband networks and establish general-purpose computerized-information services have, with very narrow exceptions, either failed outright or massively under-delivered on their promises.

The problems with their intended remedies, however, do not invalidate every concern critics of the status quo raise. The question of equal access to virtual spaces, for example, is an important issue that’s worth addressing. One major function of government in a free society is to ensure that everyone has some opportunity to participate in that society. Internet access may not be a human right in the way Sanders and company construe it, but an American who cannot access virtual public spaces is missing out on a sizeable portion of the nation’s civic life. In recognition of this reality, access to telecommunications technology has remained a public-policy priority for the federal government since the New Deal; it currently takes the form of the Universal Service Fund. While this method has its flaws and may prove difficult to scale, targeted and relatively generous programs to facilitate virtual-space access for the poor and the underserved deserve expansion.

National-security concerns in virtual spaces are also legitimate. Insofar as Facebook and LinkedIn are comparable to public places like Times Square or Wrigley Field, it’s inarguable that the government is just as obligated to protect them from security threats as it is their physical
counterparts. Likewise, in the same way government labors to protect our roads, airports, and railways from criminals and terrorists, it has an obligation to protect critical internet infrastructure and the Americans who use it. While it might not cause the same degree of physical damage as a terrorist attack on a physical space, an attack on a vital component of America’s internet infrastructure—even if privately owned—could have devastating effects on American society.

But the reality of the problem doesn’t mean that the proposed solutions, from either the left or the right, make sense. When it comes to access, a free market that has successfully brought the internet to over 90% of the population—and to 97% of those under age 50—is not failing. Government action to expand internet access would be to fix something that isn’t broken. Furthermore, while legitimate national-security concerns exist with regard to virtual-space infrastructure, there are response options available that avoid excessive government intervention or ownership.

Public resources are best spent helping those who genuinely need them. Ideally, public spending also empowers these same individuals to make consumer choices in a relatively free market. This is the thinking behind cash-assistance efforts like the Temporary Assistance for Needy Families program, the Earned Income Tax Credit, and more targeted programs like the Supplemental Nutrition Assistance Program (formerly known as “food stamps”), Section 8 housing vouchers, and existing Universal Service Fund subsidies that help people buy and pay for telephone and internet access. Direct-to-consumer subsidies that ensure access for anyone who wants it are smart public policies in a nation where virtual space is crucial to private and civic life.

On the issue of national security, demanding the government control private internet infrastructure because someone might try to disrupt it is as absurd as demanding public ownership of iconic office towers on the basis that they are attractive targets for a terrorist attack. The fact that virtual public spaces have real national-security implications should not automatically make them public property any more so than is the case with physical public spaces.

Private-property rights to public places, however, are not absolute. The two major exceptions that exist in the physical world—non-discrimination and law-enforcement-access laws—ought to exist in the virtual one as well. If the owners of a social-media platform or
other major virtual space were to exclude people from the platform on the basis of race or some other protected characteristic, civil-rights enforcers would have an obligation to come down on them with the same force they would apply to a movie-theater owner who did the same thing. While it’s important not to give law enforcement too much power to surveil the online world (as some post-9/11 laws arguably did, or as calls for encryption backdoors seek now), it’s also important to make sure that laws keep up with technology and don’t tie the hands of those trying to protect the public. Police should be able to walk around the virtual “block,” monitor what goes on in public, and obtain search warrants when they have reasonable suspicions that crimes are being planned or committed. Yet, as is the case in the physical world, they should not be given the keys and passwords, respectively, to every home and email account.

In sum, with some modest tweaks, the largely private system of ownership central to America’s physical public spaces should work well in the virtual world, too.

**Free Speech in Virtual Space**

After he incited a riot that resulted in several deaths, damaged the U.S. Capitol, and delayed the electoral vote count, a number of social-media platforms blocked then-president Donald Trump from their sites. At almost the same time, the right-leaning, conspiracy-oriented social-media site Parler found itself removed from major app stores and was subsequently shut down by its web-hosting provider before being restored a few months later. This came on the heels of efforts by major online retailers and platforms that some on the right found offensive: Conservative commentator Dennis Prager saw some of his videos demonetized on YouTube, and Amazon stopped carrying confederate-flag merchandise, to name two examples.

For many, all this was proof positive of systemic bias against those who lean right. Within days of Trump’s ban, conservative leaders called for a breakup of the major tech platforms on the grounds that they censor conservative speech. “Free speech was controlled like this in East Germany and the Soviet Union,” they wrote, “[t]his should not be happening in America.” On his way out of office, Trump himself demanded a repeal of a key internet law—Section 230 of the Communications Decency Act of 1996—that offers a degree of liability protection to these
platforms. The preceding year, he issued an executive order aimed at doing the same thing. Later, he filed a lawsuit contending that these platforms are state actors for purposes of the First Amendment.

While understandable in some respects, these efforts are almost entirely wrongheaded. The standards some sought to overturn are the same ones that apply to physical public spaces. They are as essential to preserving political discourse and the free exchange of ideas online as they are in the physical world.

Section 230, for one, simply stipulates that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” It further allows private entities to set content standards by stating that such platforms cannot be held liable for “any action voluntarily taken in good faith to restrict or ban user-generated “material that the provider or user considers to be obscene…or otherwise objectionable, whether or not such material is constitutionally protected.” These are the same rights possessed by an owner of a physical public space. Booksellers, for instance, cannot be sued for carrying certain books—even when those books are found defamatory—any more than they can be sued for refusing to carry others. Section 230 isn’t some special right or privilege granted to Big Tech moguls, but a codification of the habits, norms, and practices that have long governed physical public forums.

The best way to understand why the standard that works in the physical world is just as essential in the virtual world is to consider the available alternatives. In place of the Section 230 standard, the law could impose a “free speech” standard on internet companies—forcing virtual public places to tolerate any expression allowed under the First Amendment. This standard would present three significant problems: It would create a legal morass, erase online property rights, and impede freedom of conscience.

A free-speech standard online would impose the greatest burdens on commercial entities. Under such a regime, online platforms would regularly face the following choice: They could either allow questionable content—such as ambiguous threats of physical violence, or media that might be considered child pornography—to be posted, or they could attempt to remove such content and risk being sued or fined for a violation of users’ free-speech rights. Even if the companies behind the major virtual venues were somehow able to fairly and consistently
enforce this standard, the challenge of monitoring the billions of posts that find their way onto these sites daily would likely render the operation of these platforms financially unviable.

On the property-rights front, if anyone can use someone else’s private, virtual property for any expressive purpose protected by the First Amendment, then that property is no longer “private” in any meaningful sense. Forcing a website to host content that it finds objectionable would be no different than forcing a privately owned event center to make its space equally available to all groups and members of the public. Such a move would effectively constitute the commandeering of that space by the public in the name of free speech and equal access. This flies in the face of America’s long-standing commitment to private-property rights and the liberties connected to them. Free citizens are only free, after all, while they retain the liberty to use their property at their own discretion.

People who insist on a First Amendment standard point to the Supreme Court’s 1980 decision in *PruneYard Shopping Center v. Robins*, which upheld the ability of California’s state constitution to establish an affirmative right to free speech on certain types of privately owned property. Putting aside the fact that *PruneYard* is not federal law, the decision was based on a finding that the mall owners had “failed to demonstrate that the ‘right to exclude others’ is so essential to the use or economic value of their property that the state-authorized limitation of it amounted to a ‘taking.’” So even if *PruneYard* applied nationally, it would apply to few, if any, websites. Owners of social-media platforms have a very strong economic interest in making sure that they provide an environment that their customers and advertisers find acceptable — in fact, providing such an environment is their primary purpose as businesses. Applying a *PruneYard*-like standard to Facebook, for example, would be equivalent to saying that theater owners had to allow anybody to use their facilities — for free — even if their activities interrupted another production.

The free-speech standard would also force the owners of virtual spaces to facilitate the speech of their users even when they disagree with it themselves. This raises the same issues that the Supreme Court considered in *Masterpiece Cakeshop v. Colorado Civil Rights Commission*. If Reddit is required to use its resources and property to give a platform to all protected speech, there is little reason to suspect that Jack Phillips, the Christian baker who opposes same-sex marriage, would be
allowed to refuse to decorate a cake for a gay wedding. Conservatives were right to object to the coercive laws to which Phillips was subjected; they should be the first to object to a free-speech standard that demands internet platforms play host to ideas and behaviors that the owners believe to be immoral.

One alternative to the free-speech standard would be to end Section 230 without imposing any new standard. This approach would likely be even worse for diversity and free expression online than other proposed solutions. Without the liability shield of Section 230, the owners and operators of online platforms would be liable for any content produced by users. Under these circumstances, no sizeable commercial enterprise could afford to facilitate robust public discussion, much less video streaming; the risks of being sued for defamation when a user attacks another in public, or even being criminally sanctioned when a user distributes child pornography, would be unmanageable. Rather than functioning like the famous Speakers’ Corner in London’s Hyde Park, now-vibrant and diverse online forums would become, in the best of outcomes, the equivalent of newspapers’ letters-to-the-editor pages.

The final alternative to Section 230 would be to create new laws and agencies authorized to regulate speech on internet forums. Such an approach may be more workable than other solutions offered. However, it is also a hallmark of authoritarian states. While courts or regulators should maintain existing speech standards that apply everywhere—such as bans on child pornography or speech that incites violence—the sheer diversity of online settings demands that the law be a minimum rather than the norm. No matter how reasonable or light-handed laws about content seemed at first, they would still chill speech. A hate-speech ban initially forbidding, say, Holocaust denial and race-supremacist propaganda in online forums could quickly morph into a ban on conventional religious views on sexuality under a left-wing government or a ban on blasphemy under a right-wing one.

Section 230 presents real challenges for preserving freedom of expression in virtual public spaces. But these are ultimately the same challenges posed by the need to preserve free expression physical public spaces. And they require largely the same response: a commitment to private-property rights, free speech, and freedom of conscience. The regulations proposed by those who feel discriminated against in our digital environments are too often a threat to all three.
It’s also worth noting that the problem conservatives are trying to solve through regulation — namely, bias against them — is not quite the obstacle they sometimes make it out to be. By some measures, conservatives do just fine at disseminating their messages online. Before the platform banned him for inciting violence, Trump was the eighth-most followed person on Twitter, behind a few celebrities and his predecessor in office, Barack Obama. As of August 2021, the Republican National Committee’s Twitter account had 2.7 million followers, compared to the Democratic National Committee’s 129,000. The National Rifle Association has more than three times the followers of the gun-control giant Everytown. Even Trump’s own campaign staff seemed to believe conservative voters were using social media on a massive scale: Despite spending and raising significantly less money overall than his Democratic challenger, Trump still outspent him on social-media advertising.

That said, the perception of bias against conservatives is not entirely unfounded. Communist organizations can create Facebook pages, for example, while fascist ones appear to be banned. More fundamentally, though, the perceived bias has an eminently rational explanation.

Platforms rely primarily on two methods to identify content that violates their policies: user reports, and the judgments of their own staff members (who both monitor content and create algorithms that do the same). With regard to the former, online-platform users tend to be younger than the population overall. This means that those interacting most frequently in virtual spaces, and thus the ones making the most reports of objectionable content, tend to skew to the political left. Some newer platforms, like the social network TikTok, tend to be used primarily by the very young: The average age on that service is 24. During the 2020 election, voters between 18 and 24 chose Biden over Trump by a margin of 65% to 31%.

With regard to staff judgment, statistics show that tech-company employees donate overwhelmingly to Democratic candidates. They also tend to live and work in areas of the country where populations lean heavily to the left, including San Francisco, Boston, northern Virginia, and Austin, Texas. This means that the people charged with identifying objectionable content on internet forums and enforcing platform policies are overwhelmingly left-leaning.

When combined, these factors form a recipe for an environment in which individuals and groups on the left receive the benefit of the doubt,
while conservative ones do not. This doesn’t mean intentional, systemic bias exists—there’s little evidence of that—but natural human tendencies to be sympathetic toward those with which one agrees make it more likely that conservative content will be flagged and taken down, while progressive content will remain standing. It also shifts controversial cases in favor of the left’s standards. Platforms have taken some steps to mitigate these biases, but a more concerted effort will probably be necessary.

Nevertheless, preserving a free market online will likely be the best strategy for conservatives in the long run. Most major online platforms exist to earn money for their stockholders, and alienating a large percentage of their user base would be a terrible business move. Does TikTok want the 31% of Gen-Z voters who support Trump to feel unwelcome on its platform? If the firm’s owners are trying to earn a profit (and they are), they do not. And they would be leaving massive amounts of money on the table if they refused to respond to legitimate criticism.

Fixing real bias requires continued engagement, along with bold, peaceful, and truthful sharing of conservative ideas and values. In the meantime, conservatives would do well to remain committed to the legal standards and traditions that preserve America’s public spaces as the forums where such engagement can occur.

**HUMBLE REGULATION**

Virtual public spaces have obvious advantages over the physical spaces they are quickly replacing. Unlike traditional spaces, virtual environments are affordable to create and maintain, and they’re readily accessible from almost anywhere in the world. The creation and stewardship of the digital public sphere has generated massive amounts of wealth and spurred tremendous technological innovation. On the whole, the virtualization of the public sphere has allowed previously unimaginable levels of safe commercial and social activity to take place, to the benefit of consumers and suppliers alike.

But the rapid transformation of our public space has not been an unalloyed good. As things stand, Americans are justifiably worried that virtual public spaces have become a threat to public safety, privacy, and free speech. Simultaneously, early proposals by federal legislators to address these concerns have led others to worry that any attempt to regulate these new public spaces will soon become a threat to private-property rights and free enterprise.
The best policies for addressing all these challenges follow from the realization that the traditional approach to public spaces in the physical world can serve society well in the virtual one. This does not mandate a commitment to the status quo or an entirely hands-off attitude from the government. In fact, an assertive public role in some areas of virtual space is important and, in certain places—such as combatting non-sex crime and working to ensure that everyone can access virtual space—government ought to do more than it does now. Nevertheless, America’s time-honored commitment to competition and private property should be regulators’ primary aim. While imperfect and unlikely to satisfy everyone, such an approach is a far better guarantor of free speech and safety in our emerging virtual public spaces than heavy-handed regulation.

As is the case with other complex, evolving entities, trying to manage America’s virtual space entirely through a single central authority—whether it be Congress or Silicon Valley—will not work in the long run. The short history of the internet has shown that seemingly dominant platforms can vanish overnight if they make a single wrong move. Inappropriate political policies, entrenched in statutes or case law, could kneecap a vital economic sector and squelch future innovation for years. Those looking to develop responsible regulations of emerging virtual spaces should do so cautiously, and learn from the traditions established and refined over centuries in America’s markets, parks, and town squares.